UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/524,358	03/14/2000	Tateo Oishi	450100-02402	8951

20999	7590	12/31/2003

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER
NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/31/2003

7

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No. ●	Applicant(s)
Office Action Summary	09/524,358	OISHI ET AL.
	Examiner	**Art Unit**	
	Andrew Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *14 March 2000*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:
   1.☐ Certified copies of the priority documents have been received.
   2.☐ Certified copies of the priority documents have been received in Application No. _____.
   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

   a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1.   Claims 1-18 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1, 6, and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by

Sasaki et al US Patent No. 6,378,071. Sasaki teaches a file access system for

encrypted data within a storage device.

3.   With regards to claims 1 and 13, Sasaki discloses encrypted means for

processing data in units of an encryption block having a predetermined data length

(Sasaki, column 4, lines 1-6), processing means for performing predetermined

processing on data in units of a processing block having a data length of a whole

multiple of the length of an encryption block (Sasaki, column 3 lines 14-16 and 52-54),

storage means for storing encrypted data (Sasaki, column 3 lines 35-37 and column 4

lines 4-6), and a control means for writing encrypted data so that data positioned in the

same encryption block is also positioned in the same processing block (Sasaki, column

4, lines 1-6).

4.   With regards to claim 6, Sasaki teaches the control means outputting data read

out into the processing means (Sasaki, column 3 lines 14-16).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 2-3, 14-15, and 18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Sasaki et al US Patent No. 6,378,071 in view of Bellovin et al US

Patent No. 5,241,599.

7.   With regards to claims 2 and 14, Sasaki as described above fails to teach the

inserting of data into the processing block in order to adjust the data length so that it

becomes a whole number multiple of the predetermined length. Bellovin teaches the

insertion of data in order to meet the predetermined length of a block (Bellovin, column

10, lines 24-30). At the time the invention was made, it would have been obvious to a

person of ordinary skill in the art to utilize Bellovin's method of inserting data because it

offers the advantage of helps prevent partition attacks against encryption keys (Bellovin,

column 9 line 54 – column 10 line 47).

8.   With regards to claims 3, 15, and 18, Sasaki fails to teach the encryption process

using the block to be encrypted and a ciphertext from the previous block. Bellovin

teaches an encryption process using the block to be encrypted and a ciphertext from

the previous block in the form of cipher-block chaining (Bellovin, column 13, lines 10-13

and 30-35).

9.   Claims 4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Sasaki et al US Patent No. 6,378,071 and Bellovin et al US Patent No. 5,241,599 as

applied to claims 3 and 15 above, and further in view of Cassagnol US Patent No.

6,385,727. Sasaki and Bellovin, teach a cluster of encrypted data stored in a storage

means (Sasaki, column 3, lines 52-55, "file"), but fail to teach the storing of values

initially used when encrypting stored in one of the processing blocks. Cassagnol

teaches the storing of values initially used (cited as whitening keys) when encrypting

stored in one of the processing blocks (Cassagnol, column 10, lines 37-52). At the time

the invention was made, it would have been obvious to a person of ordinary skill in the

art to utilize Cassagnol's method of storing initial values because it offers the advantage

of allowing keys to be stored with and thus imported with their respective encrypted

blocks (Cassagnol, column 10, lines 49-52) and helps preserve memory resources by

reducing the need for on chip memory storage of keys (Cassagnol, column 10, lines 40-

47).

10.   Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Sasaki et al US Patent No. 6,378,071, Bellovin et al US Patent No. 5,241,599, and

Cassagnol US Patent No. 6,385,727 as applied to claim 4 above, and further in view of

Yuenyongsgool US Patent No. 6,202,152. Sasaki, Bellovin, and Cassagnol, as

described above, fail to teach the storage of blocks at consecutive addresses.

Yuenyongsgool teaches the storage of data by consecutive addresses (Yuenyongsgool,

column 2, lines 38-45). At the time the invention was made, it would have been obvious

to a person of ordinary skill in the art to utilize Yuenyongsgool's method of consecutive

address storage because it offers the advantage of helping accelerate information

transfers from encrypted memory (Yuenyongsgool, column 2, lines 4-23).

11.   Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki et

al US Patent No. 6,378,071 in view of Grabon et al US Patent No. 5,943,421. Sasaki, as

described above, fails to teach the data being compressed and the processing means

expanding the data read from the storage means. Grabon teaches a processor having

compression and encryption circuitry. Grabon teaches the reading of compressed data

and the processor expanding that data (Grabon, column 5, lines 1-3). At the time the

invention was made, it would have been obvious to a person of ordinary skill in the art to

utilize Grabon's compression/decompression mechanism because it offers the

advantage of increasing the data processing system speed by reducing the volume of

data that must be transferred and reducing the numbers of page faults that occur

(Grabon, column 3, lines 1-8).

12.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki et

al US Patent No. 6,378,071 in view of Bahout et al US Patent No. 5,594,793. Sasaki,

as described above, fails to teach a system for mutual identification between the

storage and data processing apparatuses. Bahout teaches a system for mutual

identification between the storage and data processing apparatuses using stored keys

and algorithms within the data processor (Bahout, column 7, lines 7-25). At the time the

invention was made, it would have been obvious to a person of ordinary skill in the art to

utilize Bahout's mutual identification method because it offers the advantage of giving

the system a degree of inviolability by ensuring that data processor only functions with a

specific storage device (Bahout, column 1, lines 9-16 and 55-60).

13.   Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Sasaki et al US Patent No. 6,378,071 in view of Bahout et al US Patent No. 5,594,793,

as applied to claim 8 above, and in further view of Bellovin et al US Patent No. ·

5,241,599.

14.   With regards to claim 9, Sasaki and Bahout, as described above fail to teach the

inserting of data into the processing block in order to adjust the data length so that it

becomes a whole number multiple of the predetermined length. Bellovin teaches the

insertion of data in order to meet the predetermined length of a block (Bellovin, column

10, lines 24-30). At the time the invention was made, it would have been obvious to a

person of ordinary skill in the art to utilize Bellovin's method of inserting data because it

offers the advantage of helps prevent partition attacks against encryption keys (Bellovin, column 9 line 54 – column 10 line 47).

15.   With regards to claim 10, Sasaki and Bahout fail to teach the encryption process using the block to be encrypted and a ciphertext from the previous block. Bellovin teaches an encryption process using the block to be encrypted and a ciphertext from the previous block in the form of cipher-block chaining (Bellovin, column 13, lines 10-13 and 30-35).

16.   Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki et al US Patent No. 6,378,071, Bahout et al US Patent No. 5,594,793, and Bellovin et al US Patent No. 5,241,599 as applied to claim 11 above, and further in view of Cassagnol US Patent No. 6,385,727. Sasaki, Bahout, and Bellovin, teach a cluster of encrypted data stored in a storage means (Sasaki, column 3, lines 52-55, "file"), but fail to teach the storing of values initially used when encrypting stored in one of the processing blocks. Cassagnol teaches the storing of values initially used (cited as whitening keys) when encrypting stored in one of the processing blocks (Cassagnol, column 10, lines 37-52). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Cassagnol's method of storing initial values because it offers the advantage of allowing keys to be stored with and thus imported with their respective encrypted blocks (Cassagnol, column 10, lines 49-52) and helps preserve memory resources by reducing the need for on chip memory storage of keys (Cassagnol, column 10, lines 40-47).

17.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki

et al US Patent No. 6,378,071, Bahout et al US Patent No. 5,594,793, Bellovin et al US

Patent No. 5,241,599, and Cassagnol US Patent No. 6,385,727 as applied to claim 11

above, and further in view of Yuenyongsgool US Patent No. 6,202,152. Sasaki, Bahout,

Bellovin, and Cassagnol, as described above, fail to teach the storage of blocks at

consecutive addresses. Yuenyongsgool teaches the storage of data by consecutive

addresses (Yuenyongsgool, column 2, lines 38-45). At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to utilize

Yuenyongsgool's method of consecutive address storage because it offers the

advantage of helping accelerate information transfers from encrypted memory

(Yuenyongsgool, column 2, lines 4-23).

Conclusion

18.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

19.   Any inquiry regarding this communication from the examiner should be directed

to Andrew Nalven at (703) 305-8407 during the hours of 7:15 AM – 4:45 PM Monday

through Thursday. The examiner can also be reached on alternate Fridays.

       In the event that attempts to reach the examiner are unsuccessful, the

examiner's supervisor, Gregory Morse can be reached on (703) 308 – 4789.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306 (for formal communications intended for entry)
**Or:**
(703) 872-9306 (for informal or draft communications, please label
"PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal
Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (703) 305-

3900.

Andrew Nalven

ALN
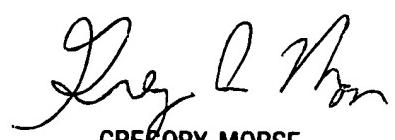
GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100